T.I.S.P./T.P.S.S.E. Community Meeting 2026

Berlin, 10. - 11.11.2026

Erkennungen und Arbeitsweisen eines SOC

Thomas Stasch, regio iT GmbH

Thomas Stasch

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- 55 Jahre alt
- Ausbildung: Verwaltungsfachwirt (AL2)
- Diplom Informatiker (FH)
- Master of Science, Wirtschaftsinformatik
- Dozent IT-Sec, Wilhelm-Büchner-Hochschule
- CISO der regio iT
- Leitung Competence Center Security



Wann brauche ich ein eigenes SOC?

SANS empfiehlt:

- Bis ca. 1.000 – 2.000 Arbeitsplätze
  Einkauf eines externen SOC (SOCaaS), da sich die betrieblichen Mindestkosten nicht wirtschaftlich darstellen lassen.
- Ca. 2.000 – 15.000 Arbeitsplätze
  Hybrid-Modell (extern + internes Kernteam)
- Ab ca. 10.000 – 15.000+ Arbeitsplätze
  Inhouse-SOC

Unser SOC ist ein Inhouse-SOC

Was verstehen wir unter einem SOC?

Ein SOC ist mehr als ein EDR auf Steroiden

Ein Security Operations Center ist die zentrale organisatorische Fähigkeit, Cyberangriffe frühzeitig zu erkennen, zu bewerten und wirksam darauf zu reagieren. Es verbindet qualifizierte Menschen, definierte Prozesse und geeignete Technologien zu einer dauerhaft handlungsfähigen Sicherheitsorganisation.

Es ist kein einzelnes Produkt, kein Tool und kein technisches Projekt.

The Invinite Game

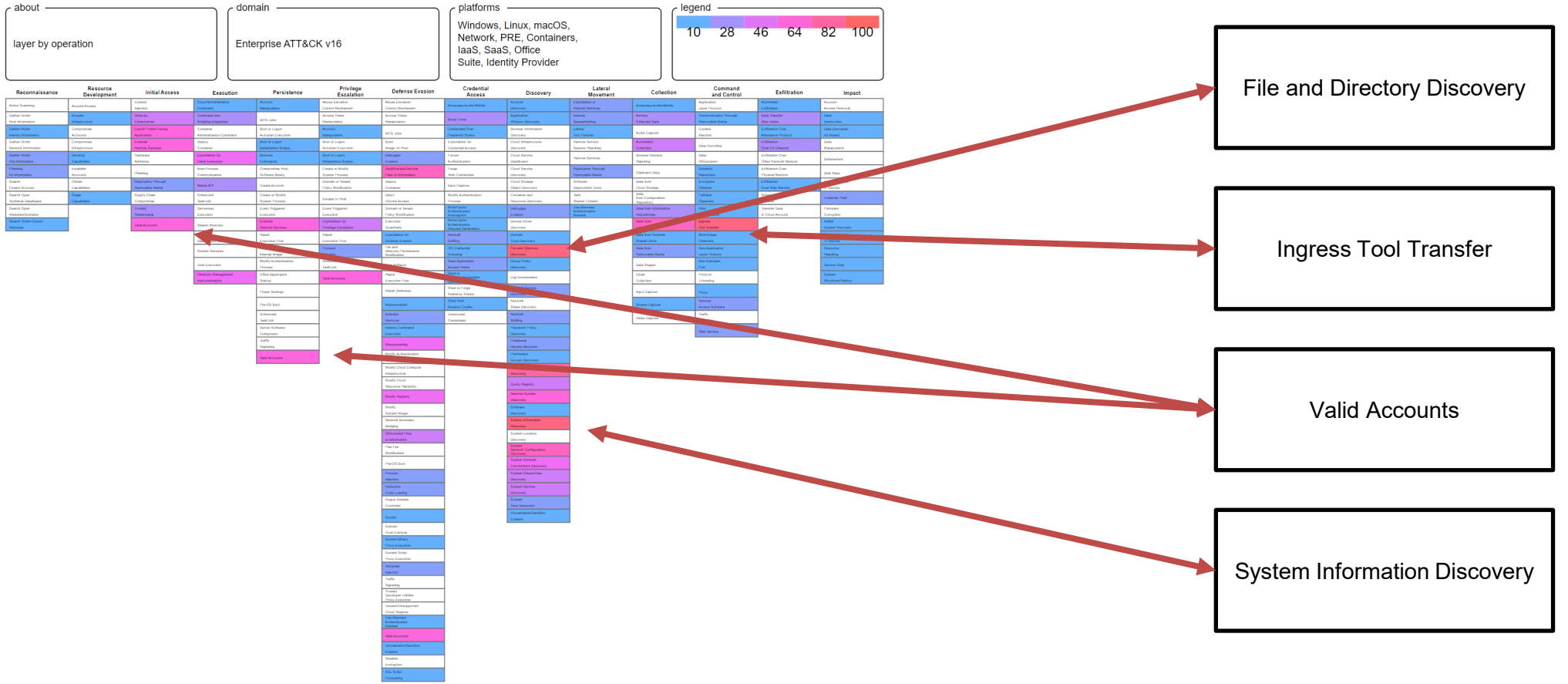


- Auf einen Marathon ausgelegt (kein Sprint)
- Kennen der „Gegner“
- Stetige Verbesserungen
- Mehrschichtige Sicherheit
- Vielzahl unterschiedlicher Detektionen
- Vorbereitung auf den Ernstfall

Security ist ein Spiel ohne Ende, ohne Gewinner und ohne Regeln!

Das Ziel lautet:
„Überleben, nicht gewinnen!“

Warum schauen wir wo hin?



Ein SOC bedeutet Multi-Layer-Security

- SIEM
- (*)DR
- Decoy-Technologien
- eigene Detection Rules
- verfügbare Analysten
- Im Idealfall:24x7
- aktive Reaktion

Sicherheit ist die Fähigkeit, Angriffe früh zu erkennen und Schäden zu begrenzen

- Vorbereiten
- Sehen
- Verstehen
- Reagieren
- Lernen

Wenn mir eine Fee erschiene…
„3 Wünsche für mein SOC“



- SIEM mit umfänglichem Logging und Handcrafted Detections
- Response auf allen Endpoints
- Red-/Blue-Teaming zur Erhöhung der Wirksamkeit

Praxisbeispiel

Samstagabend: Security Alert durch einen Honeypot:

- Gegen 21:30 wurden Portscans aus einem Kundennetz in Richtung eigener Netze detektiert
- Erste Analysen waren beunruhigend: Es gab Login-Versuch aus dem Kundennetz auf eigene Ressourcen
- Durch Zufall konnte der Sicherheitsbeauftragte des Kunden erreicht werden.
- Es stellte sich raus, dass ein beauftragter Pen-Tester „über seine Befugnisse hinaus“ versucht hatte auf fremde Ressourcen zuzugreifen.
- Wäre der ISB nicht erreichbar gewesen, wäre die Netzverbindung mit allen Diensten gegen 22:00 terminiert worden.

Praxisbeispiel

Security Alert auf einem Endgerät:

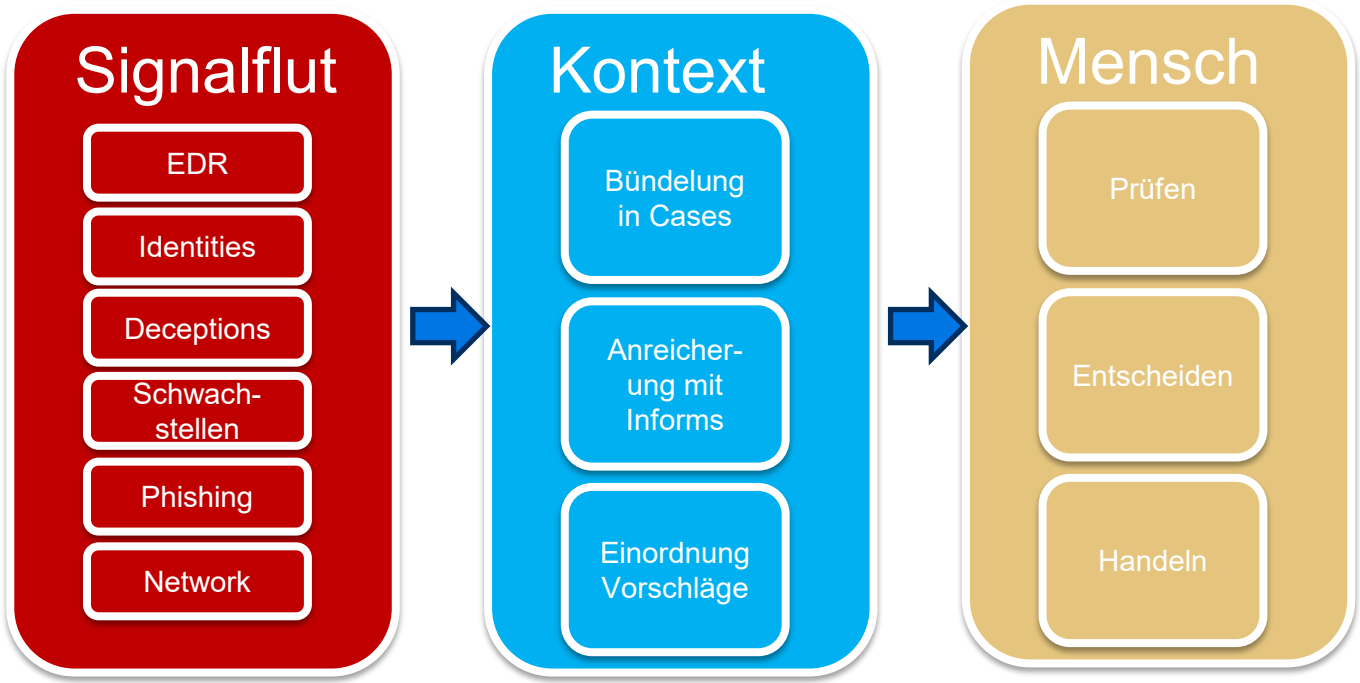
- Ein selbstentwickelter Köder auf einem dienstlichen Gerät wurde getriggert.
- Anmeldeversuch im AD mit Userdaten/Passwort aus dem Arbeitsspeicher des Benutzers wurde registriert.
- Mittels der Software „nRemoteNG“ wurden mehrere (erfolglose) Zugriffsversuche vom betroffenen System initiiert.
- Das System wurde eingezogen, mittels verschiedener Tools untersucht. Benutzerkennungen wurden zurück gesetzt. Das System wir neu aufgesetzt.

Und dann nutzen die „Bösen“ auch noch KI

- **Social Engineering**
  personalisierte Sprache, Übersetzung, Rollen- und Kontextbezug
- **Täuschung**
  synthetische Stimmen, Bilder und Identitäten
- **Reconnaissance**
  schnellere Auswertung öffentlich verfügbarer Informationen
- **Vulnerability Research**
  Unterstützung bei Analyse, Priorisierung und Codeerstellung
- **Automation**
  mehr Varianten, mehr Ziele, kürzere Iterationszyklen

Die Angreifer sind nicht intelligenter geworden - nur produktiver

Wir können aber auch KI nutzen



Kontakt

Thomas Stasch

thomas@stasch.de

thomas.stasch@regioit.de

https://www.linkedin.com/in/thomasstasch/

„Sicherheit ist wie ein Wettrennen gegen Geister

–

du siehst sie nicht, aber wenn du stehenbleibst, holen sie dich ein.“